

## El Día a Día del Administrador de Sistemas: HTTP Antivirus Proxy

# LA LÍNEA DE FUEGO

Los navegadores viven en continuo peligro de ser contagiados por un sitio web peligroso. Un proxy intermedio combinado con un antivirus puede ayudar.

**POR CHARLY KÜHNAST**

**R**ecientemente un amigo estaba planificando un viaje, e intentó navegar por un sitio web que contenía información de una ciudad importante de Alemania. Esto bien podría parecer una coincidencia o un defecto de carácter, quién sabe, pero de lo que no cabe duda es de que se equivocó tecleando la URL. El motivo: la página a la que accedió inmediatamente intentó atacar una vulnerabilidad de su navegador. Una posible solución, además de las actualizaciones regulares, y de la que con toda seguridad ya habrán oído hablar antes, es un proxy antivirus como HAVP [1].

## Un Proxy Antivirus

La instalación de un Proxy HTTP Antivirus se hace con un simple `configure && make && make install`. Hay que especificar el antivirus, que tiene que estar pre-instalado, en el paso `configure`.

En este caso, he optado por el antivirus ClamAV, elección que me proporciona una línea de comandos parecida a la siguiente: `configure --with-scanner=libclamav`.

Se sugiere la creación de un usuario y un grupo para HAVP:

```
useradd havp; groupadd havp
```

Bajo el directorio HAVP hay un subdirectorio `etc`; y bajo éste, las subcarpetas `havp` y `init.d`. La última contiene los scripts de arranque/parada que he cambiado al `/etc/init.d`. Luego he tecleado `cp -r havp /etc/` para copiar la carpeta `havp` a la ruta correcta. Entre otras cosas, la carpeta contiene un fichero de configuración principal, `havp.conf`. El siguiente paso fue borrar la línea:

## SYSADMIN

**Dispositivos de Bloque de Red ..... 58**

*Mejor rendimiento para clientes sin disco con un dispositivo de bloque de red.*

REMOVETHISLINE  
deleteme

El autor de HAVP añadió esta línea para asegurarse de que los usuarios realmente se detienen a echarle un vistazo al fichero de configuración.

## Terapia de Grupo

El siguiente paso será configurar HAVP para que se ejecute con la cuenta del usuario `havp` y configurarlo como miembro del grupo `havp`. La configuración para distintos antivirus se encuentra localizada más abajo en el fichero de configuración.

He optado por usar `libclamav` y dejarlo por defecto, aunque se puede refinar más tarde. Por supuesto, HAVP tiene una característica de registro, así configuro el directorio `/var/log/havp` y asigno permisos de escritura al usuario `havp`:

```
mkdir /var/log/havp
chown havp /var/log/havp
```

Seguidamente necesito un directorio para que HAVP almacene temporalmente los ficheros mientras los analiza. Montaré una partición vacía en este directorio, ya que HAVP necesita un sistema de ficheros que soporte bloqueos obligatorios y no sólo un directorio.

Desafortunadamente, no tengo una partición de más, así que, de momento, tendré que conformarme con un disco RAM. Esta configuración está bien para las pruebas, pero no es la idónea para un sistema de producción, ya que un disco RAM no le dará bastante espacio en el que ejecutarse. Allá vamos:

```
mkdir /var/tmp/havp
chown havp /var/tmp/havp
mkfs.ext3 /dev/ram0
```

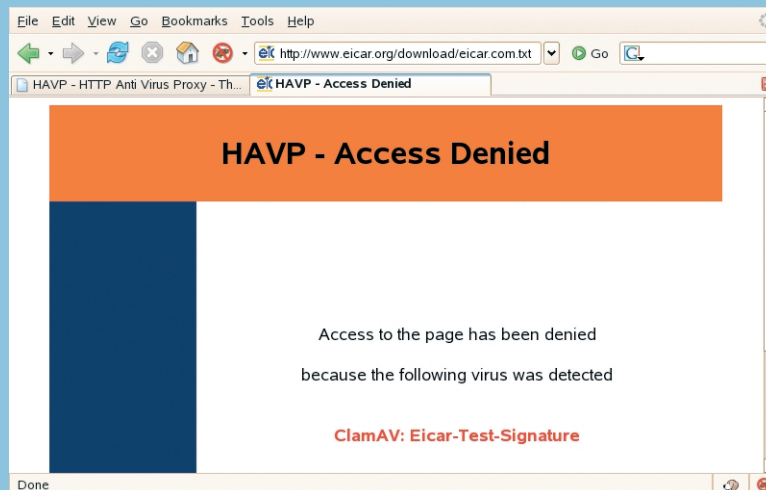


Figura 1: Si su navegador tropieza con un lugar peligroso, HAVP le alejará del peligro.

```
mount /dev/ram0 /var/tmp/havp
-o mand
```

Con esto debería estar ejecutándose HAVP, pero parece que no tengo suerte. Cuando se lanza la herramienta, me dice que aún no he editado `havp.conf`, lo que por supuesto, no es cierto.

La respuesta a este dilema está oculta en el script de inicio, que se encuentra en `/usr/local/etc/` como la ruta al fichero de configuración. Tras arreglar este problema con el script de inicio, HAVP ya está listo. Por defecto, HAVP escucha en el puerto 8080. Tras configurar Firefox para que use este puerto, es hora de hacer una prueba. Cuando intento descargar la prueba del virus EICAR, HAVP me avisa de que no puedo seguir, tal y como puede verse en la Figura 1. ¡Bien hecho HAVP!

## RECURSOS

[1] HAVP: <http://www.server-side.de>

## EL AUTOR

Charly Kühnast es Gerente de Sistemas Unix en el centro de datos de Moers, Alemania, cerca del conocido Rhin. Entre sus labores se incluye la seguridad del cortafuegos, la disponibilidad y cuidado del DMZ (zona desmilitarizada).

